Remarks

The applicants respectfully request reconsideration in view of the following comments.

Claim Objections

The drawings were objected to for failing to illustrate a "postal authority." Because the term "postal authority" no longer appears in the claims, the applicants respectfully submit this objection is moot.

Rejections under 35 USC §112 and 101

Claims 157-167 were rejected as being hybrid claims. While the applicants disagree with this rejection because the previously pending claims did not positively recite steps the performance of which was necessary for infringement, the applicants have included new claims that are plainly directed to a system. The applicants respectfully submit that, because the new claims do not positively require the performance of any method step to infringe, these claims are not in hybrid format. The applicants therefore respectfully request that the rejection be withdrawn.

Rejections under 35 USC §103

Claims 157-167 were rejected under 35 U.S.C. § 103(a) as being anticipated by Moore (U.S. 5,917,925) in view of Gordon et al (U.S. 6,527,178). The applicants respectfully submit that neither Moore nor Gordon disclose all of the elements of the new claims 168-179.

A. Claim 168

Regarding independent claim 168, Moore and Gordon both fail to disclose multiple limitations of the claims. For instance, both Moore and Gordon fail to disclose "a vendor-controlled centralized postage-issuing computer system" having "a tracking identification string allocation module programmed to allocate a unique tracking identification string to one of the end user computers in response to a tracking identification string request from the one end user

computer."

1) Moore

In direct contradiction to the claim language, Moore teaches that the ID string (construed as the unique tracking identification string) is allocated by the host computer 14 (construed as the end user computer) and not by the control computer 12 (construed as the vendor-controlled centralized postage-issuing computer system) in response to any tracking identification string request from the host computer 14. After the control computer 12 "enables a specific number" of indicia to be printed by the host computer 14 (col. 11, ll. 45-48; col. 12, ll. 55-56), the host computer 14 then "establishes" an appropriate ID string for the indicia mark and interfaces with a local encryption unit 15 to "generate" a data matrix symbology which represents the ID string (col. 11, ll. 50-56 and col. 12, line 65 – col. 13, line 10). Thus, allocation of the alleged tracking identification string is performed by the host computer 14 and not the control computer 12.

Furthermore, as will be explained below, Moore teaches that the host computer 14 must be the entity that allocates the alleged tracking identification string because this string contains confidential "customer specific" data that needs to be protected from inproper access by the control computer 12.

Moore teaches that "customer-specific" data be stored on the host computers 14 instead of the control computer 12:

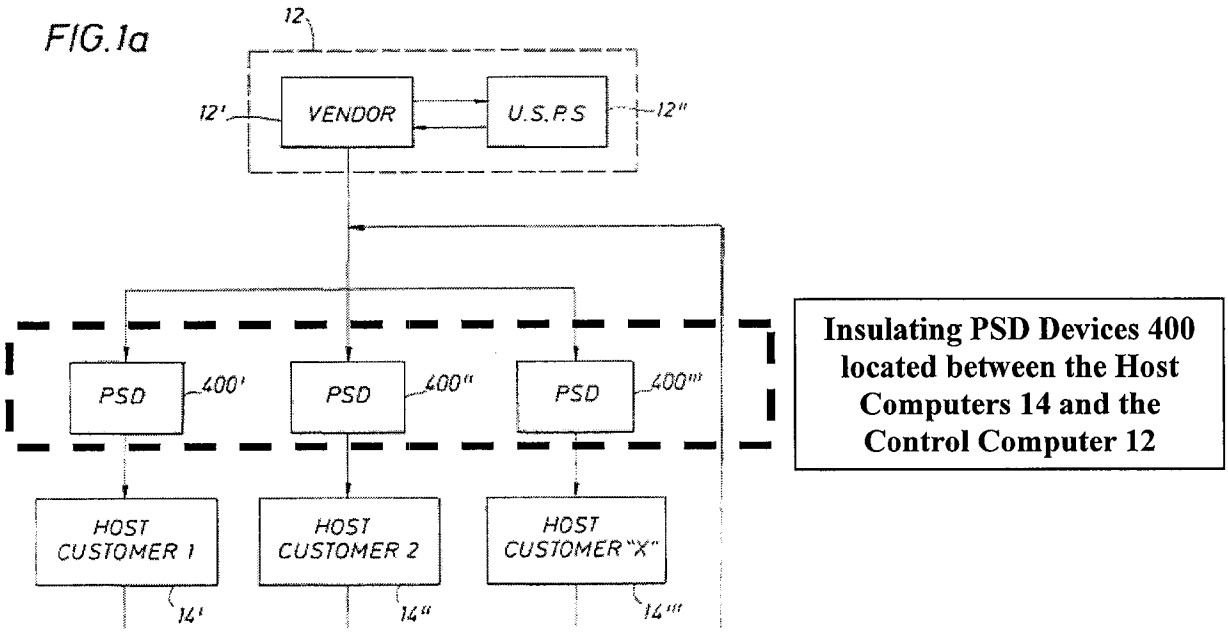
> All information contained in the indicia mark is used on site, ***transmitted back to the appropriate host computer if the information pertains directly to the customer or is "customer specific"***, or transmitted back to the control computer 12 if the information pertains to the postal service operation or even the vendor's operation. (Col. 11, ll. 12-17)(emphasis added).

> ***The single host computer is identified by the numeral 14, and stores the selected, customer specific information conveyed by the indicia mark*** and directs the indicia

printing system 16 to incorporate that information into the indicia mark on the mailpiece module. (Col. 11, ll. 25-30)(emphasis added).

Moore strives to insulate this confidential "customer-specific" data from improper access. Moore achieves this by partitioning the host computers 14 from the control computer 12 with a postal security device (PSD) 400 (e.g., an enigma card). As Moore states:

"Furthermore, ***the PSD units <u>insulate</u> the plurality of host computers from the control computer 12 so that <u>confidential</u> <u>information</u> from one host computer controlled by one company can not be clandestinely or inadvertently transferred to the host computer of another company via the control computer.***" (Col. 10, ll. 42-47)(emphasis added).



Thus, the purpose of postal security device 400 is to protect confidential information relating to the customer (i.e., the customer-specific data) on each host computer 14 from being improperly accessed by other host computers 14. This is significant because Moore teaches that

the protected "customer-specific" data is used to generate the ID string at the host computer 14. As Moore states in col. 17, lines 5-9, "***[e]ach character (e.g., ID string) represents particular information which is stored in the host computer 14. This serialized marking with selected customer specific data (unique count, plant, destination, date, lot or order)*** [sic] is printed in the I.D. Matrix format" (emphasis added).

Thus, Moore explicitly teaches away from the claimed configuration (i.e., a tracking identification string allocation module within the vendor-controlled computer system) since the allocation of the information used to generate the ID string is confidential "customer-specific" data that must remain at the host computer 14 where it is insulated from the control computer 12 by the postal security device 400.

2) Gordon

Gordon fails to disclose multiple limitations of claim 168. Among others, Gordon does not disclose "a vendor-controlled centralized postage-issuing computer system" having "a tracking identification string allocation module programmed to allocate a unique tracking identification string to one of the end user computers in response to a tracking identification string request from the one of the end user computers" because Gordon is limited only to the use of sequential serial/transaction numbers that are automatically assigned to every indicia by every party.

Gordon states that "[i]t is a further aspect of the instant invention that the postage indicia printed by a user contain a serial or transaction number. It is an additional aspect of the instant invention that the log generated from the postage indicia contain both the serial or transaction number of the postage indicia as well as the recipient address information of the mailpiece onto which that postage indicia is affixed" (col. 2, ll. 51-58). Gordon maintains these serial/transaction numbers in a master log database. When referencing this master log database, discrepencies in the form of duplicate serial/transaction numbers indicate potential unauthorized use of the indicia. However, this system can only identify unauthorized use if every indicia

created by every party is automatically assigned a unique serial/transaction number.

In contrast, claim 168 is directed to the use of unique tracking identification strings that are not automatically assigned to every indicium. As recited in the claims, the tracking identification string allocation module is programmed to allocate a unique tracking identification string to one of the end user computers in response to a tracking identification string request from the end user computer. The tracking identification string is not automatically assigned to every indicium by every party. Further, Gordon does not allocate tracking identification strings in response to end user tracking string requests distinguishable from the postage indicium request. Therefore, Gordon fails to disclose the language of claim 168.

B. Claim 179

In addition to the aforementioned claim limitations, claim 179 recites:

"The vendor-controlled centralized postage-issuing computer system of claim 168, wherein the postage indicium generation module is programmed to generate the unique postage indicium, wherein the unique postage indicium comprises ascending register information relating to the an account of the end user computer, date information, and a digital signature of the ascending register information and date information, the vendor-controlled centralized postage-issuing computer system further comprising:

> a postage indicia validation module programmed to validate the retrieved unique postage indicium and comprising a digital signature submodule programmed to verify the digital signature of the retrieved unique postage indicium with a public key; and
>
> a communications module programmed to transmit, over the communications interface, an indication of whether the unique postage indicium is valid to the USPS computer system."

Again, both Moore and Gordon fail to disclose this claim language.

1) Moore

At the outset, Moore fails to disclose digital signatures and thus cannot disclose the limitations of claim 179 pertaining thereto. But beyond this serious shortcoming, Moore teaches a system that requires any validation of customer-specific data be done at the host computer 14. However, in claim 179, the vendor-controlled computer system is programmed to validate customer-specific data. Specifically, claim 179 requires the vendor-controlled system to validate the unique postage indicium and includes a digital signature submodule that verifies the digital signature with a public key. This verified digital signature includes ascending register information of an account of the end user computer and date information. For instance, Moore explicitly identifies date information of the indicium as being an example of the protected "customer specific" data (see, e.g., col. 17, lines 5-9).

As described above, Moore teaches that customer-specific data be stored at the host computer 14 and not at the control computer 12. A PSD 400, in the form of an enigma card, insulates the host computers 14 from the control computer 12 to prevent improper access of the customer-specific data contained within the host computer 14. Moore states that any validation of customer-specific data therefore must take place at the host computer 14:

> "The control computer 12 ***and the host computer 14 receive the data from the field reader***, and interfaces with the encryption unit 15 where the message is decoded and converted to clear text. . . . ***The control computer then searches the database to validate the indicia mark and any other postal service specific information. The host computer reads and validates any customer specific information.*** Once validated, both the control and the host computers send messages back to the field reader 18 . . ." (col. 12, ll. 25-36)(emphasis added).

Claim 179 therefore clearly distinguishes from Moore. Furthermore, the applicants respectfully note that the claimed system provides significant advantage over that described by Moore. In Moore, any validation of customer-specific data must occur at the host computer 14. This means that the USPS offloads the validation of customer-specific data onto computers

belonging to the customer, e.g., personal computers at the customer's place of business. Thus, Moore essentially requires the customer to loan processing time on his or her computer to the USPS so that the USPS can perform any postage validation of customer-specific date. This could be considered a significant interference with the customer's ability to do business. The system claimed by claim 183, on the other hand, requires no such interference with the customer, since the vendor-controlled system is configured to validate customer-specific data.

2) Gordon

Gordon likewise fails to disclose the limitations of claim 183 described in the preceding section. Although Gordon discloses digital signatures, Gordon fails to disclose a vendor-controlled system programmed to validate a unique postage indicium retrieved in response to the USPS postage indicium request and fails to disclose a "digital signature submodule programmed to verify the digital signature of the retrieved unique postage indicium with a public key."

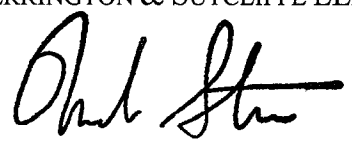
CONCLUSION

The applicants respectfully submit that independent claim 168 and the claims dependent therefrom, are allowable over the cited references. Prompt and favorable action on the merits of the claims is earnestly solicited. Should the Examiner have any questions or comments, the undersigned can be reached at (949) 567-6700.

The Commissioner is authorized to charge any fee which may be required in connection with this Amendment to deposit account No. 15-0665.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP



Dated: February 12, 2009

By:_____
Mark Stirrat
Reg. No. 50,756

ORRICK, HERRINGTON & SUTCLIFFE LLP
4 Park Plaza, Suite 1600
Irvine, CA 92614-2558
Tel. 949-567-6700
Fax: 949-567-6710
Customer Number: 34313